

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

FILED

JAN 10 2019

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
One (1) black Samsung Galaxy S9+ cellular telephone seized from
Sean Clarke McCain

Case No.

19-mj-11-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A":

located in the Northern District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2422(b)	Attempted Coercion and Enticement

The application is based on these facts:

See Affidavit of TPD Sergeant Jeremy Noland, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: January 10, 2019 2:15 p.m.

City and state: Tulsa, OK Tulsa, Oklahoma


Applicant's signature

Jeremy Noland, SGT TPD, TFO HSI
Printed name and title


Judge's signature

Paul J. Cleary, U.S. Magistrate Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeremy Noland, a Task Force Officer (TFO) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I, Jeremy Noland, have been employed by the Tulsa Police Department since January 2006. I have been a task force officer with Homeland Security Investigations (HSI) since February 2018. I am assigned to the HSI Resident Agent in Charge (RAC) Office in Tulsa, Oklahoma. Within this office, I conduct investigations in numerous areas of federal law to include, but not limited to child exploitation. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) including those on computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2422(b), and am authorized by the Attorney General to request a search warrant.

2. In 2003, your affiant graduated from Wichita State University in Wichita, Kansas, with a Bachelor's Degree in Sports Administration. In 2006, your affiant graduated from the Tulsa Police Department Police Academy. The Tulsa Police Academy course curriculum included criminal law involved in many facets of criminal investigations, drug identification, physical surveillance, preparation for prosecution, Fourth Amendment searches, drafting search warrant affidavits and what constitutes probable cause.

3. During my tenure as a criminal investigator, your affiant has participated as a case agent and support officer in numerous investigations covering various areas of criminal law. During these investigations, your affiant has participated in interviewing witnesses and

cooperating sources regarding these various crimes, and your affiant has read official reports of similar interviews by other officers. Your affiant has participated in surveillance operations, observing and recording movements of persons involved in criminal activity. Your affiant has authored search warrants and other court orders in furtherance of criminal investigations your affiant has participated in. Additionally, your affiant has spoken to other officers who have experience with child exploitation cases. Your affiant has learned that people who communicate with children online often save and maintain images and conversation data on their electronic devices for substantial periods of time. Moreover, your affiant is a federal task force officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2422(b).

4. This affidavit is submitted in support of an application for a search warrant for the device specifically described in Attachment A of this Affidavit, specifically a Samsung Galaxy S9+ cellular telephone (herein after the “SUBJECT DEVICES”) for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2422 (b), (enticement of a minor to engage in sexual activity); which item is more specifically described in Attachment B of this Affidavit.

5. The statements in this affidavit are based in part on information provided by HSI Tulsa, the Tulsa Police Department), and my assistance with the investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth only the facts that your affiant believes are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2422(b),

(enticement of a minor to engage in sexual activity); are presently located on the SUBJECT DEVICE.

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of the following:
 - a. Title 18, United States Code, Section 2422(b) prohibit a person from knowingly using the mail of any facility or means of interstate or foreign commerce to persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:
 - a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
 - b. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers,

mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); any device that can be used to connect to the Internet including a router and a modem; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates

what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

g. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

h. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the

Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion

into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
THE INTERNET, AND EMAIL**

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in children interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store in excess of 300 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage

devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. A device known as a router in conjunction with a modem allows numerous computers to connect the Internet and other computers through the use of telephone, cable, or wireless connection. A router, in conjunction with a modem, can connect literally millions of computers around the world. Routers often store information as to which computer used a modem to connect to the Internet at a specific time and location. This information when viewed along with the traces or “footprints” can provide valuable information on who distributed and/or received a visual depiction of a minor engaged in sexually explicit conduct and who possessed and accessed with intent to view a visual depiction of a minor engaged in sexually explicit conduct.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

9. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, your affiant knows that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. Your affiant also knows that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer

hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or

“keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

10. Based on your affiant’s experience and your affiant’s consultation with other agents and officers who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data

(whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

11. Additionally, based upon your affiant's training and experience and information relayed to me by agents and others involved in the forensic examination of computers, your affiant knows that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, your affiant knows that individuals who have set up either a secured or

unsecured wireless network in their residence are often among the primary users of that wireless network.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

12. On 12-18-2018 at approximately 1128 hours Detective Eric Leverington with the Tulsa Police Cyber Crimes Unit began an undercover chat investigation utilizing the Whisper social media application.

13. During the undercover investigation Detective Leverington used the persona of a fourteen-year-old female named "Abby."

14. Detective Leverington posted a general message to everyone on the Whisper app that stated, "Can't wait to move away from home and do what I want...."

15. Within one minute of posting the general message on Whisper, a subject using screen name "Tech_Sequence" responded to the message stating "what are you doing now."

16. "Tech_sequence" then asked Abby how old she was and Detective Leverington responded by saying that Abby was fourteen years of age.

17. During the conversation "Tech_sequence" asked Abby the age of the oldest guy she hung out with and then asked if she was a virgin. When Abby told "Tech_sequence" that she was just hanging out at home he stated "oh wish you could with me." When Abby stated, "you are more experienced than me," "Tech_sequence" stated "I'll teach you."

18. When Abby stated that she did not want to get pregnant, "Tech_sequence" stated "Yeah no if we were to have sex its safe sex it ruin both of our lives."

19. During the conversation “Tech_sequence” made comments like, “So did your panties get wet today?” and “So do u shave yet idk when that starts lol.”

20. When Abby said she was nervous about meeting, “Tech_sequence” stated “No need be nervous ill take u home with me then ill drop u off where u want after we done hanging out.”

21. When Abby said again that she was afraid of getting pregnant, “Tech_sequence” stated, “I understand and we will use condoms”. “Tech_sequence” then stated, “Yeah im not going to hurt you I don't want to go to jail.”

22. During the conversation “Tech_sequence” asked Abby what she had done sexually and then told her that he enjoyed “licking pussy.” When Abby told him that she had never done that before he stated, “OK well you will tomorrow.”

23. During the conversation “Tech_sequence” repeatedly asked Abby to send him “naughty” or “sexy” photos via the whisper app.

24. On 12-20-2018 at approximately 0959 hours Abby agreed to meet “Tech_sequence” at a church in the area of 100 S Vandalia Ave.

25. When Investigators observed a blue Honda civic circling the area it was stopped for a routine traffic violation. When Investigators approached the vehicle, they identified the driver as Sean Clarke McCain, W/M, DOB: 5-29-1987.

26. When McCain was asked why he was in the area he admitted that he was meeting someone. Investigators placed McCain under arrest after he was positively identified from a photo he sent to Abby.

27. McCain was placed into a vehicle and read his Miranda warning. McCain agreed to speak to Investigators and signed a written rights waiver.

28. During the video recorded interview McCain admitted that he utilized the Whisper app to communicate with a female named Abby that he knew was fourteen years of age. McCain admitted that he told Abby via chat that he wanted to “eat her out” and would use condoms when they had sexual intercourse. McCain admitted that he knew what he was doing was illegal and that he should go to jail. McCain also admitted that he deleted all communications with Abby from his phone as officers were pulling him over. The SUBJECT DEVICE was recovered from McCain’s vehicle.

29. Your affiant knows that McCain used the SUBJECT DEVICE to communicate using the application Whisper. As stated above, your affiant knows that this application is most commonly run on cellular telephones, such as the SUBJECT DEVICE. Your affiant asserts that McCain stated he deleted the application from the SUBJECT DEVICE and the data can possibly be recovered by an examiner using forensic software/hardware.

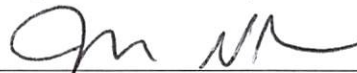
CONCLUSION

19. Based upon the above-described facts and circumstances, your affiant believes that a search warrant served upon the SUBJECT DEVICE will aid law enforcement in locating evidence that McCain utilized the SUBJECT DEVICE to entice what he believed was a minor victim to engage in sexual intercourse with him.

20. Therefore, your affiant asserts there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the

device described in Attachment A. Your affiant respectfully requests that this Court issue a search warrant for the device described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

21. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Jeremy Noland, Sergeant Tulsa Police
TFO Homeland Security Investigations

Sworn and subscribed before me this 10th day of January, 2019.



PAUL J. CLEARY
UNITED STATES MAGISTRATE JUDGE

Attachment A

The items to be searched are

One (1) black Samsung Galaxy S9+ cellular telephone; Model: SM-G965U;
IMEI: 356420094875739

Attachment B

Information, correspondence, records, documents, or other materials pertaining to the enticement or coercion of minors to engage in sexual acts or sexual conduct, as defined in 18 U.S.C. 2422(b), that were transmitted or received using the cellular device.

Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof.

Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using the cellular device.

Records of other items which evidence ownership or use of the device described in Attachment A.